

**METHOD AND APPARATUS FOR
CONTROLLING E-MAIL ACCESS**

5

BACKGROUND OF THE INVENTION
Field of the Invention

10 The present invention relates generally to e-mail messaging systems, and, particularly, to a system and methodology for controlling access to e-mail data content present in e-mail messages.

Discussion of the Prior Art

15 20 25

Senders of E-mail messages often want the message to be retrieved and accessed by the intended recipient and not made available to anybody else to access. For example, a sender of an e-mail message including content of an intimate or personal nature would like to prevent a receiving user from showing his/her note to other people. Standard prevention methods that include encryption only helps to prevent unauthorized access to data while it is being communicated over the communication medium, e.g., phone lines. These security methods however, cannot prevent improper 25 use of messages at a receiving end after they are decrypted.

It would thus be highly desirable to provide a system and method that enables a sender to control access to e-mail data after sending the e-mail message to the intended recipient.

5

Summary of the Invention

It is an object of the present invention to provide a system and method for enabling a sender to control access to e-mail and electronic information content after sending the e-mail message to an intended recipient.

10

According to a preferred embodiment of the invention, there is provided a system and method for controlling access to electronic information packages including e-mail messages communicated from a sending device to a device at one or more destination locations. The system and method includes determining fulfillment of one or more conditions at the destination location; and, implementing controls in response to detection of a fulfilled one or more conditions to enable access to content provided in a communicated package. The access includes enabling a user to perform certain operations (e.g., playing, displaying) on the package content at the destination location, or, preventing certain operations from being performed (e.g., copying, saving). A mechanism is included for enabling automatic

20

destruction of the e-mail messages immediately after being read by an authorized recipient, or, after a predetermined time interval from receipt of the message. A verification system is additionally employed enabling a sender to verify and 5 authenticate users attempting to access the e-mail at the destination location prior to authorizing use or playback of the e-mail message.

Brief Description of the Drawings

10 Further features, aspects and advantages of the apparatus and methods of the present invention will become better understood with regard to the following description, appended claims, and accompanying drawings where:

15 Fig. 1 is a general block diagram depicting the system for controlling e-mail access by senders.

20 Fig. 2 is a diagram illustrating how a sender controls access to his/her message at a receiving computer terminal.

Fig. 3 is an illustration depicting the window shell e-mail message according to the invention.

Fig. 4 is an illustration depicting the electronic information package to be sent by the sender.

5 Fig. 5(a) is an illustration depicting the method implemented for remote authorization according to the invention.

Fig. 5(b) is an illustration depicting the method implemented for local authorization according to the invention.

10 Fig. 6 is an illustration depicting the general workflow process performed at the receiver terminal.

Detailed Description of the Preferred Embodiment

15 Figure 1 is a general block diagram depicting the system 10 for controlling e-mail access by senders. As shown in Figure 1, the system implements electronic devices for sending one or several electronic information packages 60 from one or several computer devices 12 at originating locations through communication channels 25a,b, such as telephone channels, wireless channels, radio links for delivery over a network, e.g., the Internet 19, to one or several computer devices 32 at destination locations. In the preferred embodiment, "electronic information packages" 60

include one or more of the following data types: e-mail messages, audio data, video data, animation data, textual data, pictorial data, which may include content of a confidential, personal, or intimate type. It is understood that an electronic information package may include any other types of data content, i.e., of a non-personal nature. According to the invention, the system enables access to these packages at the destination points and controls access to these packages at destination points by allowing or forbidding certain operations to be performed on these packages at these destination points in accordance with predetermined conditions. That is, only if certain predetermined conditions at these destination points are fulfilled, access to or destruction of these information packages is enabled.

10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95

20

It is understood that computer devices 12, 32 at originating and destination locations are devices that comprise CPU and memory storage devices (not shown) however, such devices 12, 32 may include: laptop/notebook computers, embedded devices, and consumer electronics (kitchen appliances, TV, electronic gadgets, palmtops, and telephones). Further, as shown in Figure 1, the sending terminal will include a memory or database storage device 14 comprising recipient verification/authentication data accessible by the sender as will be described herein.

As shown in Figure 1, the computer device 32 at the destination location includes a modified e-mail program or executor 47 for retrieving and notifying a recipient of a retrieved message. The recipient computer device 32 further includes a controller module 35 implementing software controls for preventing certain operations 37 from being performed on received electronic information packages in accordance with the invention as discussed herein. Such controls include the satisfaction and/or determination of one or more certain conditions, as will be described in greater detail herein. Particularly, the controller module 35 permits or prevents one or more of the following operations to be performed on the received electronic information packages: a saving operation for saving these packages in memory storage devices at destination points; a transfer operation such as copying, printing, storing or downloading of these packages and data to memory storage devices; a displaying operation for video data, text, picture and animation data on one or several display devices (not shown) at destination points; and, playing audio data on one or several audio playback/speaker devices 38 at destination points (as shown in Figure 1). It is understood that other operations such as the destruction of the received electronic package may be enabled or prevented by controller module 35. Alternately, the electronic information package

itself may be equipped with a program that is capable to control access to its content and destroy these packages when certain conditions are fulfilled. Thus, for instance, a sender system 5 may be equipped with a program that is capable of controlling access to its content and destroy these packages when the certain conditions are fulfilled.

10 In a preferred embodiment, an electronic information package may be automatically destructed at the destination computer terminal 32 at a pre-determined time after it is received. Thus, as shown in Figure 1, a message destroyer process 46 which may be executing as part of the controller module, or separately therefrom, implements a timer mechanism 43 for determining time elapsed from receipt of the electronic information package at computer device 32. After one or more pre-determined time intervals has elapsed, the message destroyer mechanism 46 will automatically trigger a destruction operation in the computer terminal for deleting the electronic information package.

20 According to the invention, the number of intervals and length of a time interval may be set by the sender of the message, for instance, as a parameter to be entered as part of the e-mail message. As will be described in greater detail herein, this parameter information is received as part of or, in addition to the e-mail message, and implemented by the message destroyer 46

and timer mechanisms at the destination device 32. The actual destruction operation may be performed by the controller module 35 separately from or, in conjunction with a particular computer operating system.

5

It is understood that other conditions may be satisfied for triggering the destruction of a received electronic information package at the destination computer terminal. The other conditions include, but are not limited to the following: a) the detection of someone or something trying to perform a forbidden operation on the received electronic information package at the computer device 32; b) the direct command from the e-mail sender to instruct the control module to destroy a message at a later point in time; c) the detection of a modification or change in the CPU; a change in memory amount, or memory modification; a modification to or change of a peripheral device implemented at computer devices at destination points that are not related to the process of displaying or playing information packages at destination points; and d) the detection of when a playback and/or display of information package content is completed at the destination computer device 32.

10
11
12
13
14
15
16
17
18
19
20

Preferably, the condition a) of detecting attempted performance of a forbidden operation on the received electronic information package at the computer device 32 may be specified by the sender and entered as a parameter in the e-mail message, or, as a data 5 attached to the message. As mentioned herein, types of forbidden operations include: a saving operation for saving these packages in memory storage devices at destination points; and, a transfer operation such as copying, printing, storing or downloading of these packages and data to memory storage devices. In operation, 10 the control module 35 either separately from or, in conjunction with the computer device's operating system, will detect such a forbidden operation attempt, and trigger the destroyer process 46 to destruct the received electronic information package.

Similarly, as for condition b) the sender may additionally send a direct command via e-mail at a later point in time as a parameter 15 in the e-mail message, or, as data or a program attached to the message in order to trigger the destroyer process 46 to destruct the received electronic information package.

20 Preferably, the condition c) of detecting a modification or change in the CPU or a change/modification of memory or peripheral device may be specified by the sender of the package and performed by the control module 35. Once such a condition is

detected, the control module will trigger the destroyer process 46 to destruct the received electronic information package.

Similarly, as for condition d) the control module 35 will trigger the destroyer process 46 to destruct the received electronic

5 information package upon detection of a second or subsequent attempt to playback and/or display information package content at the computer device 32.

Still other conditions may be satisfied for triggering the destruction of a received electronic information package at the destination computer terminal. As shown in Figure 1, the other conditions include, but are not limited to the following: e) the detection of one or several processes running in CPU or memory devices at destination points 32 that are related to process of copying, downloading, printing, or saving information packages, or, f) the detection of pressing a certain key on a keyboard device 28, the pressing of a button, or the attempted use of other input devices (e.g., a speech recognition device, or a pen-table) at destination locations. As described above with respect to conditions c) and d), the detection of conditions e) and f) are performed by the control module 35 in conjunction with the computer's operating system, which cooperatively functions to

trigger the destroyer process 46 to destructure the received electronic information package at the receiver device 32.

In addition to specifying types of conditions for triggering the destruction of a received electronic information package at the destination computer terminal, the sender may specify one or more additional sets of conditions that must be satisfied for enabling the performance of certain operations on the received electronic information package at the destination location. As mentioned herein, types of permitted operations that may be performed include: but are not limited to, the following: a displaying operation for video data, text, picture and animation data on one or several display devices (not shown) at destination points; and, playing audio data on one or several audio playback/speaker devices 38 at destination points. The other conditions include, but are not limited to the following: g) a permission from the sender, e.g., entered as a parameter in the e-mail message, or, as a data or program attached to the message for use by the control module; and, h) the detection and identification of authorized user(s), for which access to these information packages is allowed; or, i) the detection or identification of other permissible electronic systems at destination locations

that are trying to perform operations on the received electronic package content.

As depicted in Figure 2, the condition h) of detecting and identifying authorized user(s) to accomplish the detection of an e-mail message, the computer device 32 at the destination location and the sending device may include the monitoring of user(s) via TV cameras or video camera devices 49 that are installed at destination points. For example, video device hardware/software devices, such as video camera 49, may be implemented to enable a sender 12 to observe users that request to read or play a content of information packages at destination points.

In a preferred embodiment, an electronic information package access operation may be enabled at the destination computer terminal 32 by implementation of a identification/authentication process 56 which executes locally as part of the controller module 35, or remotely therefrom. The identification/authentication process 56 that enables users or systems to access information packages may be performed in accordance with one or more of the following methods: the presentation by a user of a "pid" (personal ID) and/or passwords;

and, the presentation and verification of that user's biometrics, fingerprints, and/or voice. That is, the identification/authorization process 56 implements well known techniques for verifying user's biometrics, fingerprints, and/or 5 detected voice patterns at computer device 32. Such techniques for verifying, identifying may include techniques such as described in commonly-owned, co-pending U.S. Patent Application No. 09/079,754 (Y0998-033 (728-103), entitled APPARATUS AND 10 METHODS FOR USER RECOGNITION EMPLOYING BEHAVIORAL PASSWORDS, the whole contents and disclosure of which is incorporated by reference as if fully set forth herein.

15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
100
105
110
115
120
125
130
135
140
145
150
155
160
165
170
175
180
185
190
195
200
205
210
215
220
225
230
235
240
245
250
255
260
265
270
275
280
285
290
295
300
305
310
315
320
325
330
335
340
345
350
355
360
365
370
375
380
385
390
395
400
405
410
415
420
425
430
435
440
445
450
455
460
465
470
475
480
485
490
495
500
505
510
515
520
525
530
535
540
545
550
555
560
565
570
575
580
585
590
595
600
605
610
615
620
625
630
635
640
645
650
655
660
665
670
675
680
685
690
695
700
705
710
715
720
725
730
735
740
745
750
755
760
765
770
775
780
785
790
795
800
805
810
815
820
825
830
835
840
845
850
855
860
865
870
875
880
885
890
895
900
905
910
915
920
925
930
935
940
945
950
955
960
965
970
975
980
985
990
995
1000
1005
1010
1015
1020
1025
1030
1035
1040
1045
1050
1055
1060
1065
1070
1075
1080
1085
1090
1095
1100
1105
1110
1115
1120
1125
1130
1135
1140
1145
1150
1155
1160
1165
1170
1175
1180
1185
1190
1195
1200
1205
1210
1215
1220
1225
1230
1235
1240
1245
1250
1255
1260
1265
1270
1275
1280
1285
1290
1295
1300
1305
1310
1315
1320
1325
1330
1335
1340
1345
1350
1355
1360
1365
1370
1375
1380
1385
1390
1395
1400
1405
1410
1415
1420
1425
1430
1435
1440
1445
1450
1455
1460
1465
1470
1475
1480
1485
1490
1495
1500
1505
1510
1515
1520
1525
1530
1535
1540
1545
1550
1555
1560
1565
1570
1575
1580
1585
1590
1595
1600
1605
1610
1615
1620
1625
1630
1635
1640
1645
1650
1655
1660
1665
1670
1675
1680
1685
1690
1695
1700
1705
1710
1715
1720
1725
1730
1735
1740
1745
1750
1755
1760
1765
1770
1775
1780
1785
1790
1795
1800
1805
1810
1815
1820
1825
1830
1835
1840
1845
1850
1855
1860
1865
1870
1875
1880
1885
1890
1895
1900
1905
1910
1915
1920
1925
1930
1935
1940
1945
1950
1955
1960
1965
1970
1975
1980
1985
1990
1995
2000
2005
2010
2015
2020
2025
2030
2035
2040
2045
2050
2055
2060
2065
2070
2075
2080
2085
2090
2095
2100
2105
2110
2115
2120
2125
2130
2135
2140
2145
2150
2155
2160
2165
2170
2175
2180
2185
2190
2195
2200
2205
2210
2215
2220
2225
2230
2235
2240
2245
2250
2255
2260
2265
2270
2275
2280
2285
2290
2295
2300
2305
2310
2315
2320
2325
2330
2335
2340
2345
2350
2355
2360
2365
2370
2375
2380
2385
2390
2395
2400
2405
2410
2415
2420
2425
2430
2435
2440
2445
2450
2455
2460
2465
2470
2475
2480
2485
2490
2495
2500
2505
2510
2515
2520
2525
2530
2535
2540
2545
2550
2555
2560
2565
2570
2575
2580
2585
2590
2595
2600
2605
2610
2615
2620
2625
2630
2635
2640
2645
2650
2655
2660
2665
2670
2675
2680
2685
2690
2695
2700
2705
2710
2715
2720
2725
2730
2735
2740
2745
2750
2755
2760
2765
2770
2775
2780
2785
2790
2795
2800
2805
2810
2815
2820
2825
2830
2835
2840
2845
2850
2855
2860
2865
2870
2875
2880
2885
2890
2895
2900
2905
2910
2915
2920
2925
2930
2935
2940
2945
2950
2955
2960
2965
2970
2975
2980
2985
2990
2995
3000
3005
3010
3015
3020
3025
3030
3035
3040
3045
3050
3055
3060
3065
3070
3075
3080
3085
3090
3095
3100
3105
3110
3115
3120
3125
3130
3135
3140
3145
3150
3155
3160
3165
3170
3175
3180
3185
3190
3195
3200
3205
3210
3215
3220
3225
3230
3235
3240
3245
3250
3255
3260
3265
3270
3275
3280
3285
3290
3295
3300
3305
3310
3315
3320
3325
3330
3335
3340
3345
3350
3355
3360
3365
3370
3375
3380
3385
3390
3395
3400
3405
3410
3415
3420
3425
3430
3435
3440
3445
3450
3455
3460
3465
3470
3475
3480
3485
3490
3495
3500
3505
3510
3515
3520
3525
3530
3535
3540
3545
3550
3555
3560
3565
3570
3575
3580
3585
3590
3595
3600
3605
3610
3615
3620
3625
3630
3635
3640
3645
3650
3655
3660
3665
3670
3675
3680
3685
3690
3695
3700
3705
3710
3715
3720
3725
3730
3735
3740
3745
3750
3755
3760
3765
3770
3775
3780
3785
3790
3795
3800
3805
3810
3815
3820
3825
3830
3835
3840
3845
3850
3855
3860
3865
3870
3875
3880
3885
3890
3895
3900
3905
3910
3915
3920
3925
3930
3935
3940
3945
3950
3955
3960
3965
3970
3975
3980
3985
3990
3995
4000
4005
4010
4015
4020
4025
4030
4035
4040
4045
4050
4055
4060
4065
4070
4075
4080
4085
4090
4095
4100
4105
4110
4115
4120
4125
4130
4135
4140
4145
4150
4155
4160
4165
4170
4175
4180
4185
4190
4195
4200
4205
4210
4215
4220
4225
4230
4235
4240
4245
4250
4255
4260
4265
4270
4275
4280
4285
4290
4295
4300
4305
4310
4315
4320
4325
4330
4335
4340
4345
4350
4355
4360
4365
4370
4375
4380
4385
4390
4395
4400
4405
4410
4415
4420
4425
4430
4435
4440
4445
4450
4455
4460
4465
4470
4475
4480
4485
4490
4495
4500
4505
4510
4515
4520
4525
4530
4535
4540
4545
4550
4555
4560
4565
4570
4575
4580
4585
4590
4595
4600
4605
4610
4615
4620
4625
4630
4635
4640
4645
4650
4655
4660
4665
4670
4675
4680
4685
4690
4695
4700
4705
4710
4715
4720
4725
4730
4735
4740
4745
4750
4755
4760
4765
4770
4775
4780
4785
4790
4795
4800
4805
4810
4815
4820
4825
4830
4835
4840
4845
4850
4855
4860
4865
4870
4875
4880
4885
4890
4895
4900
4905
4910
4915
4920
4925
4930
4935
4940
4945
4950
4955
4960
4965
4970
4975
4980
4985
4990
4995
5000
5005
5010
5015
5020
5025
5030
5035
5040
5045
5050
5055
5060
5065
5070
5075
5080
5085
5090
5095
5100
5105
5110
5115
5120
5125
5130
5135
5140
5145
5150
5155
5160
5165
5170
5175
5180
5185
5190
5195
5200
5205
5210
5215
5220
5225
5230
5235
5240
5245
5250
5255
5260
5265
5270
5275
5280
5285
5290
5295
5300
5305
5310
5315
5320
5325
5330
5335
5340
5345
5350
5355
5360
5365
5370
5375
5380
5385
5390
5395
5400
5405
5410
5415
5420
5425
5430
5435
5440
5445
5450
5455
5460
5465
5470
5475
5480
5485
5490
5495
5500
5505
5510
5515
5520
5525
5530
5535
5540
5545
5550
5555
5560
5565
5570
5575
5580
5585
5590
5595
5600
5605
5610
5615
5620
5625
5630
5635
5640
5645
5650
5655
5660
5665
5670
5675
5680
5685
5690
5695
5700
5705
5710
5715
5720
5725
5730
5735
5740
5745
5750
5755
5760
5765
5770
5775
5780
5785
5790
5795
5800
5805
5810
5815
5820
5825
5830
5835
5840
5845
5850
5855
5860
5865
5870
5875
5880
5885
5890
5895
5900
5905
5910
5915
5920
5925
5930
5935
5940
5945
5950
5955
5960
5965
5970
5975
5980
5985
5990
5995
6000
6005
6010
6015
6020
6025
6030
6035
6040
6045
6050
6055
6060
6065
6070
6075
6080
6085
6090
6095
6100
6105
6110
6115
6120
6125
6130
6135
6140
6145
6150
6155
6160
6165
6170
6175
6180
6185
6190
6195
6200
6205
6210
6215
6220
6225
6230
6235
6240
6245
6250
6255
6260
6265
6270
6275
6280
6285
6290
6295
6300
6305
6310
6315
6320
6325
6330
6335
6340
6345
6350
6355
6360
6365
6370
6375
6380
6385
6390
6395
6400
6405
6410
6415
6420
6425
6430
6435
6440
6445
6450
6455
6460
6465
6470
6475
6480
6485
6490
6495
6500
6505
6510
6515
6520
6525
6530
6535
6540
6545
6550
6555
6560
6565
6570
6575
6580
6585
6590
6595
6600
6605
6610
6615
6620
6625
6630
6635
6640
6645
6650
6655
6660
6665
6670
6675
6680
6685
6690
6695
6700
6705
6710
6715
6720
6725
6730
6735
6740
6745
6750
6755
6760
6765
6770
6775
6780
6785
6790
6795
6800
6805
6810
6815
6820
6825
6830
6835
6840
6845
6850
6855
6860
6865
6870
6875
6880
6885
6890
6895
6900
6905
6910
6915
6920
6925
6930
6935
6940
6945
6950
6955
6960
6965
6970
6975
6980
6985
6990
6995
7000
7005
7010
7015
7020
7025
7030
7035
7040
7045
7050
7055
7060
7065
7070
7075
7080
7085
7090
7095
7100
7105
7110
7115
7120
7125
7130
7135
7140
7145
7150
7155
7160
7165
7170
7175
7180
7185
7190
7195
7200
7205
7210
7215
7220
7225
7230
7235
7240
7245
7250
7255
7260
7265
7270
7275
7280
7285
7290
7295
7300
7305
7310
7315
7320
7325
7330
7335
7340
7345
7350
7355
7360
7365
7370
7375
7380
7385
7390
7395
7400
7405
7410
7415
7420
7425
7430
7435
7440
7445
7450
7455
7460
7465
7470
7475
7480
7485
7490
7495
7500
7505
7510
7515
7520
7525
7530
7535
7540
7545
7550
7555
7560
7565
7570
7575
7580
7585
7590
7595
7600
7605
7610
7615
7620
7625
7630
7635
7640
7645
7650
7655
7660
7665
7670
7675
7680
7685
7690
7695
7700
7705
7710
7715
7720
7725
7730
7735
7740
7745
7750
7755
7760
7765
7770
7775
7780
7785
7790
7795
7800
7805
7810
7815
7820
7825
7830
7835
7840
7845
7850
7855
7860
7865
7870
7875
7880
7885
7890
7895
7900
7905
7910
7915
7920
7925
7930
7935
7940
7945
7950
7955
7960
7965
7970
7975
7980
7985
7990
7995
8000
8005
8010
8015
8020
8025
8030
8035
8040
8045
8050
8055
8060
8065
8070
8075
8080
8085
8090
8095
8100
8105
8110
8115
8120
8125
8130
8135
8140
8145
8150
8155
8160
8165
8170
8175
8180
8185
8190
8195
8200
8205
8210
8215
8220
8225
8230
8235
8240
8245
8250
8255
8260
8265
8270
8275
8280
8285
8290
8295
8300
8305
8310
8315
8320
8325
8330
8335
8340
8345
8350
8355
8360
8365
8370
8375
8380
8385
8390
8395
8400
8405
8410
8415
8420
8425
8430
8435
8440
8445
8450
8455
8460
8465
8470
8475
8480
8485
8490
8495
8500
8505
8510
8515
8520
8525
8530
8535
8540
8545
8550
8555
8560
8565
8570
8575
8580
8585
8590
8595
8600
8605
8610
8615
8620
8625
8630
8635
8640
8645
8650
8655
8660
8665
8670
8675
8680
8685
8690
8695
8700
8705
8710
8715
8720
8725
8730
8735
8740
8745
8750
8755
8760
8765
8770
8775
8780
8785
8790
8795
8800
8805
8810
8815
8820
8825
8830
8835
8840
8845
8850
8855
8860
8865
8870
8875
8880
8885
8890
8895
8900
8905
8910
8915
8920
8925
8930
8935
8940
8945
8950
8955
8960
8965
8970
8975
8980
8985
8990
8995
9000
9005
9010
9015
9020
9025
9030
9035
9040
9045
9050
9055
9060
9065
9070
9075
9080
9085
9090
9095
9100
9105
9110
9115
9120
9125
9130
9135
9140
9145
9150
9155
9160
9165
9170
9175
9180
9185
9190
9195
9200
9205
9210
9215
9220
9225
9230
9235
9240
9245
9250
9255
9260
9265
9270
9275
9280
9285
9290
9295
9300
9305
9310
9315
9320
9325
9330
9335
9340
9345
9350
9355
9360
9365
9370
9375
9380
9385
9390
9395
9400
9405
9410
9415
9420
9425
9430
9435
9440
9445
9450
9455
94

destination points are permissible electronic systems. It is understood that the permissible electronic systems may be specified by a sender, e.g., entered as a parameter in the e-mail message, or, as a program attached to the message or information package.

5

According to the invention, access to electronic information packages is provided on displays 31, or, via speakers 38 or telephone sets 39, as shown in Figure 1. As shown in Figure 3, 10 electronic information packages comprising visual, text, image, and/or pictorial data are displayed through window shells 59 according to known e-mail format or GUI representations, such as provided by Lotus Notes, Netscape, Microsoft Outlook, Eudora, and the like. However, it is understood that the window shell 59 will only display e-mail message content and prevent any further 15 operations from being performed (no printing, copying, etc.). For instance, textual and pictorial data in window shells 59 may run from beginning of the data to the end (from one end of the window shell to another).

20

In accordance with the invention as illustrated in Figure 4, an electronic information package 60 may comprise one or more of the following fields: 1) a reading time field 62 having a data

structure which specifies the time in hours, minutes and seconds (HH:MM:SS) for when the message content is to be displayed or available for the recipient; 2) a Valid time interval field 64 (from <date:time> to <date:time>) which specifies the time range during which the message content may be read, i.e., if it is accessed before the specified time, the message will not be available, if expired, it will be automatically destroyed; 3) an authentication method field 66 which includes a description of the method implemented (either remotely or locally) for authenticating the recipient/user; 4) authentication data field 68 which includes data used for the verification method implemented, e.g., voice pattern, fingerprint and other biometric data; 5) the target recipient(s) field 70 which specifies one or more recipients allowed to access the message and their e-mail addresses; 6) a Sender field 72 which includes information about the person/system that sends the message; and 7) the actual body of the message 80, i.e., electronic information content.

The system for providing remote user authentication, according to the invention, is now described in view of Figure 5(a). As shown in Figure 5(a), at step 82, the message package is created on the sender system 12 and sent to the receiver terminal via communications channels 25. Preferably, the entire communication

between the sending and receiving end-points is encrypted. At step 84, at the destination 32, the receiver device processes the authentication method field 66 from the message package 60 and determines the type of the authentication method and that the authentication is to be performed remotely. After obtaining data (e.g., by obtaining a user-entered userid or password, and/or a camera image, voice-print, or a finger-print scan, etc.), the collected information is communicated back to the sender device at step 85 for processing there. Then, at step 86, a verification of identity is be done by a query to the database 14 (Figure 1), visual inspection (by the active video camera system (Figure 2), or by using apparatus for user recognition according to techniques known in the prior art. When all the verification conditions are fulfilled, at step 88, the sender will either grant the access to the information by sending a message, or, otherwise it may send a request to destroy the message. If authentication is successful, the message package will be available to the recipient for the period of time specified in Reading Time field 62 (Figure 4), as indicated at step 89, otherwise it will be destroyed, as indicated at step 90.

The system for providing local user authentication, according to the invention, is now described in view of Figure 5(b). As shown

in Figure 5(b), at step 92, the message is created on the sender system 12. Further this step 92 requires determining a list of authorized recipient(s) and the authentication method, and the retrieval of authentication data from the database 14 (Figure 1) at the sender terminal. Once all this information is determined and all the data required for authentication is packaged with the message in the Authentication Data field 68, the message is then sent to the recipient terminal where it is received at step 94. At step 94, the authentication takes place and the results are compared with the data from the Authentication Data field 68. A decision is made at step 95 to determine if the authentication was successful. If the authentication was successful, the message becomes available to the recipient for the period of time specified in reading time field at step 96, otherwise it is destroyed at step 98.

It should be understood that, local authentication is much faster than remote authentication, because, after the message is sent, it executes independent of the sender.

Figure 6 is a workflow diagram illustrating the method executed at the receiver device for controlling e-mail access of the invention. As indicated at a first step 102, the message package

is received. Regardless of the type of the authentication specified in Authentication Method field 66, the receiver enables the authentication method at step 104 and compares the results with the data contained in Authentication Data field 68 of the received message, as indicated at step 106. If the authorization fails as indicated at 108, the destroy process is executed and the message content is destroyed. Likewise, if the validation fails as indicated at 110, the destroy process is executed. If the validation is accepted, the message content is available for display/playback. Once the message is displayed or played back, the reading time (HH:MM:SS) message field is checked and the timer mechanism invoked to enable display/playback of the message content for the specified time interval, as indicated at 118. If the reading message time has elapsed, as indicated at 115, the destroy process is executed and the message content destroyed. Likewise, the valid time interval is checked at 118 to determine if the recipient has accessed the message content within the valid time period indicated by the Valid time field 64 of the message. Once the valid time interval has elapsed as indicated at step 120, the message content is destroyed. Further, as shown in Figure 6, any illegal operation 121 causes the message to be destroyed and the sender to be optionally notified at step 123. Thus, a message is available to the recipient only when

successfully authenticated and only within the time period
specified in Reading Time field.

While the invention has been particularly shown and described
5 with respect to illustrative and preformed embodiments thereof,
it will be understood by those skilled in the art that the
foregoing and other changes in form and details may be made
therein without departing from the spirit and scope of the
invention which should be limited only by the scope of the
10 appended claims.

1234567890 - 012345678901234567890